CVE-2015-1521

描述：analyzer/protocol/dnp3/DNP3.cc in Bro before 2.3.2 does not reject certain non-zero values of a packet length, which allows remote attackers to cause a denial of service (buffer overflow or buffer over-read) via a crafted DNP3 packet.

软件：bro-master

源码：src/analyzer/protocol/dnp3/DNP3.cc

出现位置： 216-229行

关键源码：

bool DNP3\_Base::AddToBuffer(Endpoint\* endp, int target\_len, const u\_char\*\* data, int\* len)

{

if ( ! target\_len )

return true;

int to\_copy = min(\*len, target\_len - endp->buffer\_len);

memcpy(endp->buffer + endp->buffer\_len, \*data, to\_copy);

\*data += to\_copy;

\*len -= to\_copy;

endp->buffer\_len += to\_copy;

return endp->buffer\_len == target\_len;

}